Protecting Sensitive Business Data in Motion

HoloNet's OnFire Delivers Real-time Anomaly Detection for a New Threat Landscape

The Challenge: Pinpointing Breaches Through the Movement of Data

The vast majority of security incidents and breaches involve the compromise or theft of sensitive business data. External actors or even rogue insiders are either stealing data, which entails moving it from one place to another, or simply accessing data they are not authorized to see. In either case, protecting sensitive business data is the primary goal of all the security measures enterprise undertake.

Now, digital transformation has created a new threat landscape. In the era of cloud-based infrastructures and global collaboration, sensitive business data flows freely across and beyond the distributed enterprise every day. Even though enterprises may deploy a number of security measures to protect networks, secure applications and detect threats, conventional solutions offer little visibility into what happens to sensitive data before, during and after a breach. Instant visibility into data movements – specifically, which data is being moved, by whom, from where to where, using what device – has been lacking until now. For enterprises to take effective breach prevention and remediation measures, they need the ability to detect any abnormal movements of data in real time.

Data Breach Detection – Where Are We Today?

Conventional cybersecurity tends to be focused on two areas: protecting the perimeter from external threats and tracking down abnormal or suspicious activity within the perimeter. If we think of an enterprise as a large gilded mansion, full of rich targets for thieves, the former would be equivalent to "guarding the gates," and the latter would mean asking unfamiliar visitors to state their business. In today's more open IT environment, however, both approaches fall short.

In the first case, the “perimeter” as we once knew it has become extremely porous and malleable. Sensitive business data flows in and out of the enterprise for entirely legitimate business purposes all the time. Meanwhile, breaching the perimeter has become the most basic step in an attack. A sophisticated cyber-thief needs to find only one vulnerability – one crack in the wall, as it were – to gain entry to an enterprise network. In spite of the millions of dollars invested in intrusion prevention, big breaches continue to occur at alarming rates. Guarding the gates is no longer enough to prevent the pilfering of treasure once the thieves have broken into the mansion.

The problem with focusing on suspicious behavior internally is that conventional breach detection yields too many false positives. Going back to our mansion metaphor, it’s a challenge for guards to distinguish uninvited guests snooping where they don’t belong from household attendants going about their business. Behavior that appears abnormal may be totally innocent. Security teams are hard pressed to investigate every instance of suspicious activity, only to find that most of them are false alarms. Unfortunately, that is the state of most breach detection efforts today. It’s a drain on both the efficiency and effectiveness of security countermeasures.

Instead of simply trying to block access to sensitive data or chase down suspected thieves after the fact, enterprises need to add an effective means of tracking the data itself as it moves internally or externally – and knowing instantly when it falls into the wrong hands.

Detecting Abnormal Movement of Data

Technology exists today that enables enterprises for the first time to gain instant visibility into data in motion and detect abnormal movement of sensitive data in real time. HoloNet’s OnFire solution provides a complete network “hologram” showing the relationships among four key security vectors - users, devices, applications and data. Through a patent-pending technology, OnFire connects each data movement with its actual user and the device and application used in real-time. Leveraging machine learning and analytics, the solution builds a complete and precise profile for each of these four vectors and the connections among them.

Fig. 1 – *OnFire provides instant visibility and anomaly detection for all sensitive data in motion through machine learning that connects users, devices, apps and data in real time.*

This multi-dimensional correlation allows OnFire to detect anomalies in data movement in real time. This significantly reduces false positive rates by enabling security teams to focus specifically on the abnormal movement of data rather than any abnormal network or application behavior. With instant, real-time anomaly detection, HoloNet's OnFire gives security teams time to take necessary preventive and remediation measures and minimize any losses or damage the breach may cause.

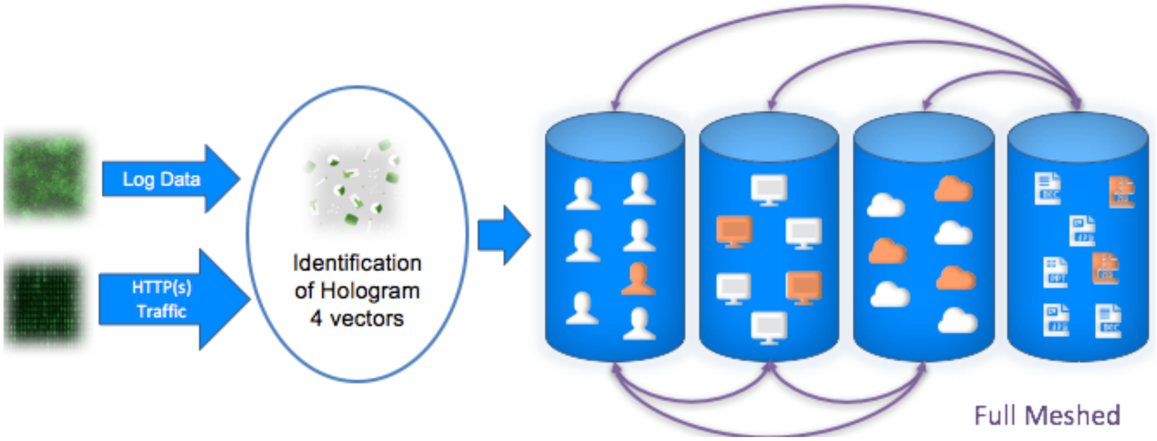

Fig. 2 - "*OnFire captures metadata fed to a Behavior Analytic Engine and generates fully-meshed holographic vectors comprised of uniquely identifiable user credentials, devices, apps and files/data.*"

Use Case: Compromise of an End-Point Computer

To better understand how OnFire detects malicious breaches, and what distinguishes it from existing solutions, consider a realistic business scenario: the CFO's laptop has been compromised by a hacker, who then tries to use the computer to steal confidential data files from inside the company network.

In a conventional security environment, the IT team has no good solution for detecting a compromised machine until the damage is done. Network-based anomaly detection solutions may be able to see suspicious activity on the network, but will likely generate too many false positives and impede the IT team's ability to respond.

With the HoloNet solution, OnFire will have profiled the CFO's laptop. Through a built-in content inspection engine, OnFire identifies the types of sensitive files the CFO typically moves, and from where – for example, financial statements from the main finance department server. OnFire links all data movements with the actual user – the CFO – and her device in real-time, and profiles that behavior accordingly. After a brief learning period, OnFire will have built a base pattern for the CFO's movement of data using her laptop.

When the hacker gets control of her laptop, he attempts to access source code from a completely different server in a different department. This is clearly out of the CFO's normal pattern. OnFire instantly detects the abnormal behavior and alerts the CFO and the security team.

Complementing the Existing Security Infrastructure

OnFire is the first security solution on the market that provides a top-down, holistic view of how sensitive business data is being transferred across corporate networks, from end-point devices to servers anywhere, either internally or externally via the Internet. This view serves as a complement to both end-point security solutions and existing network-based security solutions. Current end-point solutions provide a very detailed and comprehensive view of everything happening at the device level, but they don't show a complete picture of how individual end-points are connected to each other and to the outside world. OnFire's top-down view across all devices and servers adds that extra dimension of visibility to existing end-point solutions. OnFire can track the movement of data to or from an end-point device without the need to install an agent on the device.

Network-based solutions may spot anomalous patterns among data traffic, but have no way of knowing whether that indicates the improper movement of sensitive data. If we compare data traffic to actual traffic, imagine that sensitive data is "gold" being transported by cars on a highway. Any car's driving pattern may change whether it is carrying the gold or not; if the security system is simply tracking changes in driver behavior, it will lead to too many false positives. OnFire complements network security solutions by showing which cars are carrying the gold, who the drivers are and where they're going. The solution effectively eliminates all false positives that are based solely on changes in driving behavior.

Perimeter defenses, network-based breach detection and end-point security are all essential components of a solid security infrastructure. However, they are not sufficient to protect the sensitive business data that thieves are really after. If an intruder manages to elude these security measures – the literal definition of a breach – then the data is at risk.

To pinpoint and thwart breaches with precision, enterprises need a last line of defense to complement their existing security infrastructure. With HoloNet's OnFire, the would-be thief is caught red-handed – betrayed by the data itself as soon as it starts to move out of its normal user, device and application patterns. In today's more open, virtualized computing environments, it enables enterprises to collaborate and share sensitive data with far less fear of compromise.

For more information about OnFire, please visit www.holonetsecurity.com

# # #